GP/~~2766~~ 2131

PATENT

#5

MJ:mgs 10/16/01 245-53434 67824

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Alexandre F. Tenca, Çetin K. Koç

Art Unit: 2766

Application No. 09/621,020

Filed: July 21, 2000

For: SCALABLE METHODS AND APPARATUS FOR MONTGOMERY MULTIPLICATION

Examiner: --

Date: October 16, 2001

CERTIFICATE OF MAILING

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being deposited with the United States Postal Service on October 16, 2001 as First Class Mail in an envelope addressed to: COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231.

Michael D. Jones
Attorney for Applicant

INFORMATION DISCLOSURE STATEMENT PURSUANT TO 37 C.F.R. § 1.97(b)(3)

TO THE COMMISSIONER FOR PATENTS
Washington, DC 20231

Sir:

Listed on the accompanying form PTO-1449 and enclosed herewith are several English-language documents. Applicants respectfully request that these documents be listed as references cited on the issued patent.

Applicants filed this Information Disclosure Statement before the mailing date of a first Office action on the merits. However, if the Patent Office determines that a fee is required for Applicants to file this Information Disclosure Statement, please charge any such fees to Deposit Account No. 02-4550. A **duplicate** copy of this Information Disclosure Statement is enclosed.

Respectfully submitted,

KLARQUIST SPARKMAN CAMPBELL
LEIGH & WHINSTON, LLP

By
Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

MJ:mgs 10/16/01 245-53434 67829

#5

INFORMATION DISCLOSURE STATEMENT **BY APPLICANT**	Docket: 245-53434	App: 09/621,020
	Applicant: Tenca et al.	
	Filed: July 21, 2000	Art Unit:

OTHER DOCUMENTS

			Menezes, J. et al., Handbook of Applied Cryptography, CRC Press, 1996, pp. 600-603.
			Even, S., "Systolic Modular Multiplication," Advances in Cryptology, Proceedings Crypto 90, Lecture Notes in Computer Science, vol. 537, A. J. Menzes et al., eds. pp. 619-624 (1991).
			Bosselaers, A. et al., "Comparison of three modular reduction functions," Advances in Cryptology, Proceedings Crypto 93, pp 175-186 (1996).
			Koç, Ç. et al., "Carry-Save Adders for Computing the Product AB Modulo N," Electron. Lett., **26**:899-900 (1990).
			Agnew, G. et al., "Arithmetic Operations in GF(2^m)," J. of Cryptology, pp. 3-13 (1993).
			Koç, Ç. et al., "Analyzing and Comparing Montgomery Multiplication Algorithms," IEEE Micro, **16**:26-33 (June 1996).
			Koç, Ç., "Montgomery reduction with even modulus," IEE Proc.-Comput. Digit. Tech., **141**:314-316 (September 1994).
			Paar, C., et al., "Fast Arithmetic Architectures for Public-Key Algorithms over Galois Fields GF($(2^n)^m$)," Eurocrypt '97, May 11, 1997, pp. 363-378.
			Leu, J., et al., "A Scalable Low-Complexity Digit-Serial VLSI Architecture For RSA Cryptosytem," in IEEE Workshop on Signal Processing Systems 1999, pp. 586-595.

EXAMINER:	DATE

*Examiner: Initial if considered, whether or not in conformance with MPEP 609; draw line through cite if not in conformance and not considered. Send copy.

MJ:mgs 10/16/01 245-53434 67829

#6

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-53434	App: 09/621,020
	Applicant: Tenca et al.	
	Filed: July 21, 2000	Art Unit:

OTHER DOCUMENTS

			Bartee, T., et al., "Computation with Finite Fields," Inform. and Control 6:79-98 (1963).
			Walter, C., "Faster Modular Multiplication by Operand Scaling," in Advances in Cryptology Proc.Crypto '91, LNCS 576, J. Feigenbaum, ed., 1992, pp. 313-323.
			Bajard, J. et al., "An RNS Montgomery Modular Multiplication Algorithm," IEEE Trans. Computers 47:766-776 (July 1998).
			Koç, Ç., et al., "Montgomery Multiplication in GF(2^k)," Designs, Codes and Cryptography 14:57-69 (April 1998).

EXAMINER:	DATE

*Examiner: Initial if considered, whether or not in conformance with MPEP 609;
draw line through cite if not in conformance and not considered. Send copy.